



QUALYS SECURITY CONFERENCE 2018

Real-Time Vulnerability Management

Operationalizing the VM process from detection to remediation

Michael Kassim,
Account Manager, Qualys, Inc.

Giorgio Gheri
Security Solutions Architect, Qualys, Inc.

Agenda

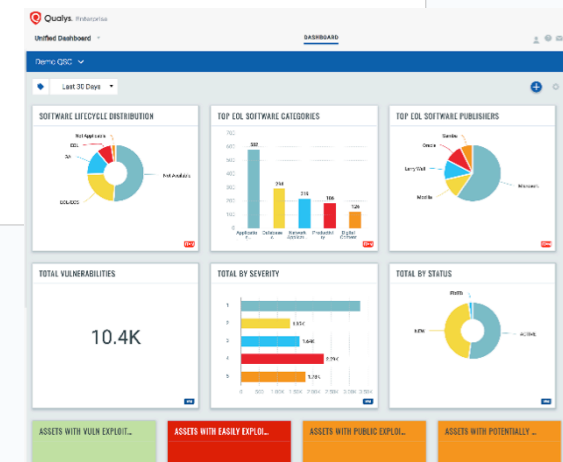
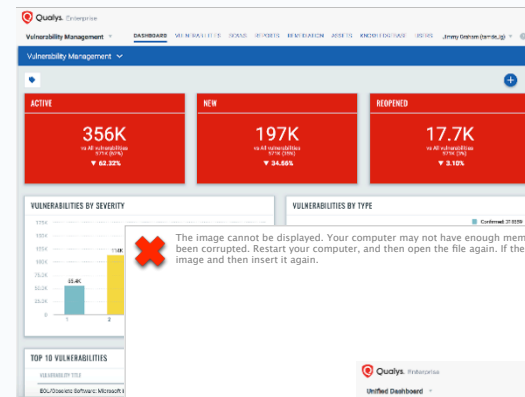
Expanding Vulnerability Management

Unified Dashboard

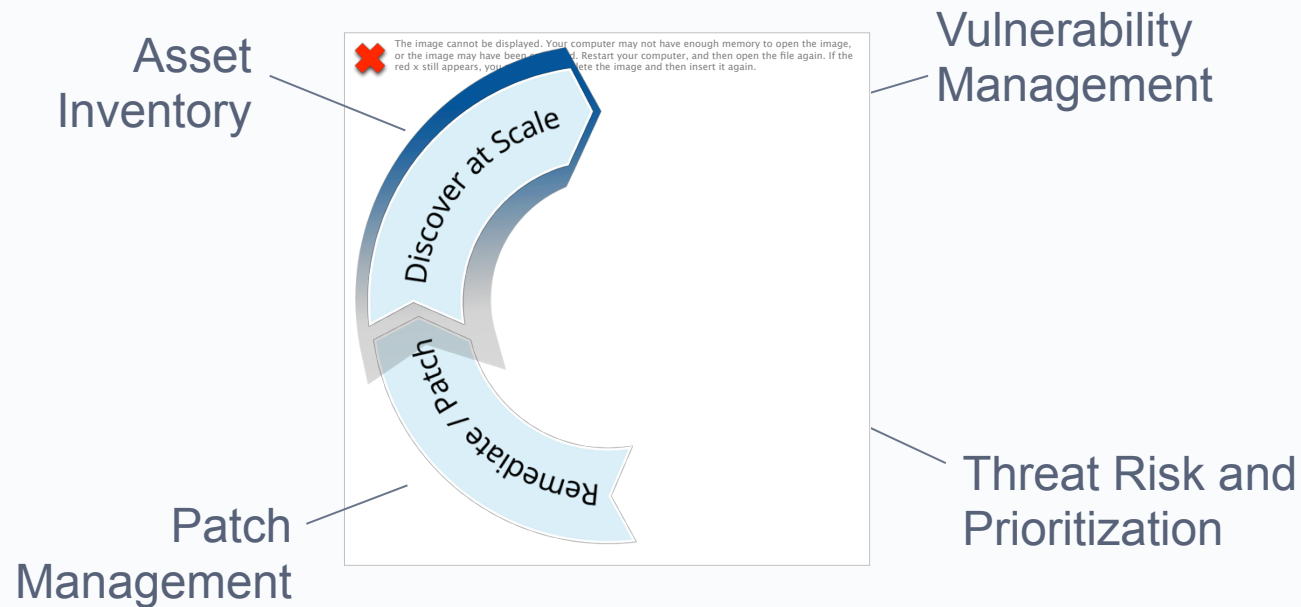
Introducing Qualys Patch Management

2 QSC
Conference,
2018

04
Decemb
2018



Vulnerability Management Lifecycle



Expanding Vulnerability Management



Vulnerability Management

Platform Evolution

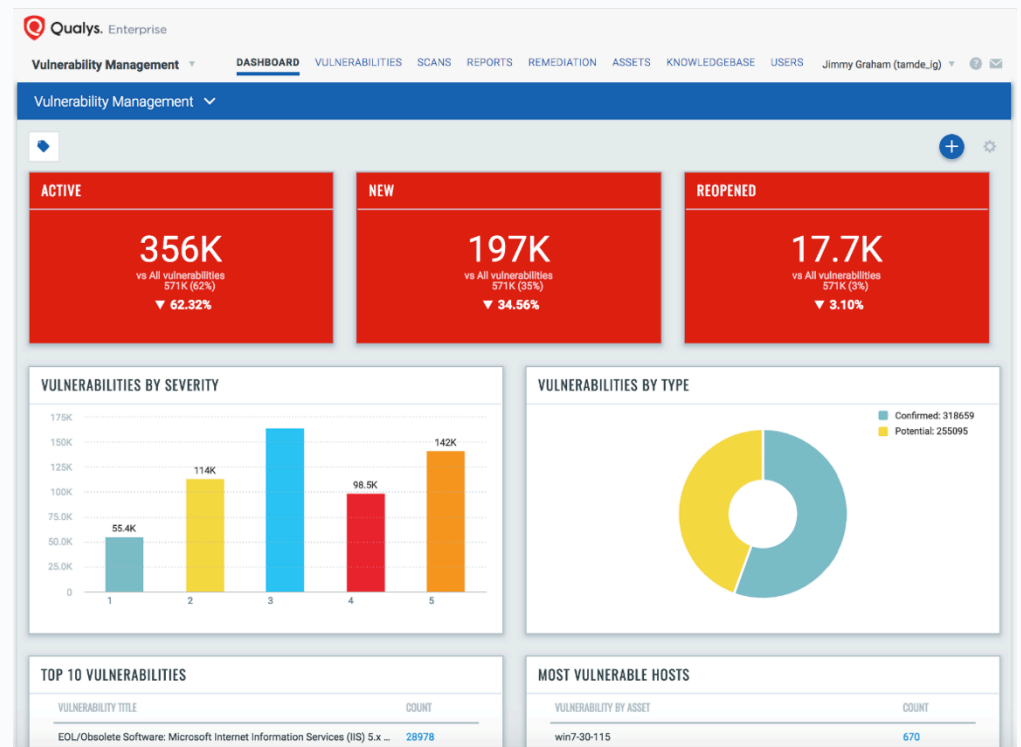
Elastic VM Dashboard

Merges AssetView
technology into Qualys VM

Build widgets with
vulnerability counts

Search filters for quickly
building queries

Replace long-running
reports with live widgets



Opening Up the VM Detections Platform

Custom Remote Detections

Qualys Remote Detection
Interface (QRDI)

Create your own or share on
Qualys Community

Supports HTTP(S) and raw TCP

Regex grouping and capturing

LUA scripting for advanced logic

```
{ IPcam_QRDI.json •
1  {
2    "detection_type": "http dialog", "api_version": 1, "trigger_type": "
3    "dialog": [
4      {
5        "transaction": "http get",
6        "object": "/cgi-bin/CGIPProxy.fcgi?usr=visitor&pwd=testingqr
7        "on_error": "stop"
8      },
9      {
10       "transaction": "process",
11       "mode": "regex",
12       "match": "<firmwareVer>(.*?)</firmwareVer>",
13       "extract": [{"var": "wholeMatch"}, {"var": "firmwareVersion"
14     },
15     {
16       "transaction": "report", "result": {"concat": ["Foscam Firm
17     }
18   ]
19 }
20
```

Demo

Assets



Elastic VM Dashboard

PATCH SUMMARY

PATCH STATUS

Assets

PATCH LOG

VMs

VMs

VMs

PATCH SUMMARY

Adobe Reader and Acrobat
Security Update

MS17-010

4019251

APP

100%

77719

CVE-2016-3427

No

2

2

CVE-2016-3427

Microsoft .NET Framework
Security Update April 2017

APSEC14-01

4019254

OS

100%

197040

CVE-2016-1980

Yes

2

3

Microsoft SQL Server 2008 R2
Service Pack 3 (KB2979597)

2979597

APP

100%

351175

CVE-2017-4371

Yes

1

1

Microsoft Windows Security
Update May 2017

MS17-014

4019253

OS

100%

197054

None

Yes

3

1

Oracle Java SE Critical Patch
Update - April 2017

MS17-014

4019253

APP

100%

170682

CVE-2016-3754

No

4

5

Security Updates for Windows
Server 2008 x64 Edition...

MS16-012

4019254

APP

100%

170682

CVE-2016-3754

No

3

5

Unified Dashboards

Overview

Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

Target servers, containers, instances, web apps, etc. using Asset Tags



Demo

Assets



Unified Dashboard Preview

Adobe Reader and Acrobat Security Update (APSB17-02)	MS17-0204	3019251	APP	None	277119	CVE-2016-3427	No	2	2
Microsoft .NET Framework Security Update April 2017	APSB17-01	3019250	OS	None	197040	CVE-2016-3427	No	2	3
Microsoft SQL Server 2008 R2 Service Pack 3 (KB2979597)		2979597	APP	None	351175	CVE-2017-4371	Yes	1	4
Microsoft Windows Security Update May 2017	MS17-004	4019263 4019264	OS	None	197054	None	Yes	3	1
Oracle Java SE Critical Patch Update - April 2017	MS17-004		APP	None	170682	CVE-2016-3751	No	4	5
Security Updates for Windows Server 2008 x64 Edition...	MS16-002		APP	None	170682	CVE-2016-3751	No	3	5

Unified Dashboard Rollout

Phase 1

Unified Dashboard App

Global dashboard filters

Support for:



Phase 2

Unified widget builder

Upgrade existing Cloud App
Dashboards

Support for:

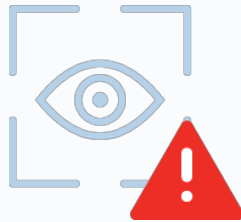


Qualys Patch Management

Overview

Current Patch Management Tools

Challenges and Impact



Manual correlation of vulnerability to patch leads to delayed mean-time-to-remediation

Waiting for vulnerability reports to confirm the patch has fixed the vulnerability

Remote systems only patched when connected to corporate network

Limited or no coverage of third-party apps

Multiple patching solutions for each OS type

Introducing Qualys Patch Management



Automated correlation of vulnerability and patch data
– Which patch fixes the CVE?

Simple dashboarding for tracking patch deployments

Patch using the Qualys Cloud Agent, anywhere

Patch OS and third-party applications

Single solution for Windows, macOS, and Linux

Shift From Reaction Mode to Operational Security



Always up-to-date on
missing patches

Security and IT teams can
“speak the same language”

Collaboration –key to
successful digital
transformation

Unify discovery, prioritization,
and remediation into one
platform

Rapid remediation of high-
profile vulnerabilities in days
vs. weeks

Regularly scheduled
deployments are repeatable
and reported on

Demo

Assets



Patch Management Beta

Adobe Reader and Acrobat Security Update (APR)	MS17-010	3013251	APP	None	777119	CVE-2016-3427	No	2	2
Microsoft .NET Framework Security Update April 2017	APSEC1-04	3013252	OS	None	197040	CVE-2016-3427	No	2	2
Microsoft SQL Server 2008 R2 Service Pack 3 (KB2979597)		2979597	APP	None	351175	CVE-2017-4371	Yes	1	1
Microsoft Windows Security Update May 2017	MS17-014	3013253 3013254	OS	None	197054	None	Yes	3	3
Oracle Java SE Critical Patch Update - April 2017	MS17-014		APP	None	170682	CVE-2016-3754	No	4	5
Security Updates for Windows Server 2008 x64 Edition...	MS16-012		APP	None	170682	CVE-2016-3754	No	3	5

Platform Support



XP SP3+
Vista

Windows 7
Windows 8/8.1
Windows 10
Server 2003 SP2+
Server 2008/R2
Server 2012/R2
Server 2016



OS X 10.10
Yosemite

OS X 10.11
El Capitan
macOS 10.12
Sierra
macOS 10.13
High Sierra
macOS 10.14
Mojave



RHEL 6,7

CentOS 5.4+,6,7

SUSE Linux
Enterprise Server/
Desktop 11,12,15

Oracle Ent Linux
6,7(Server)

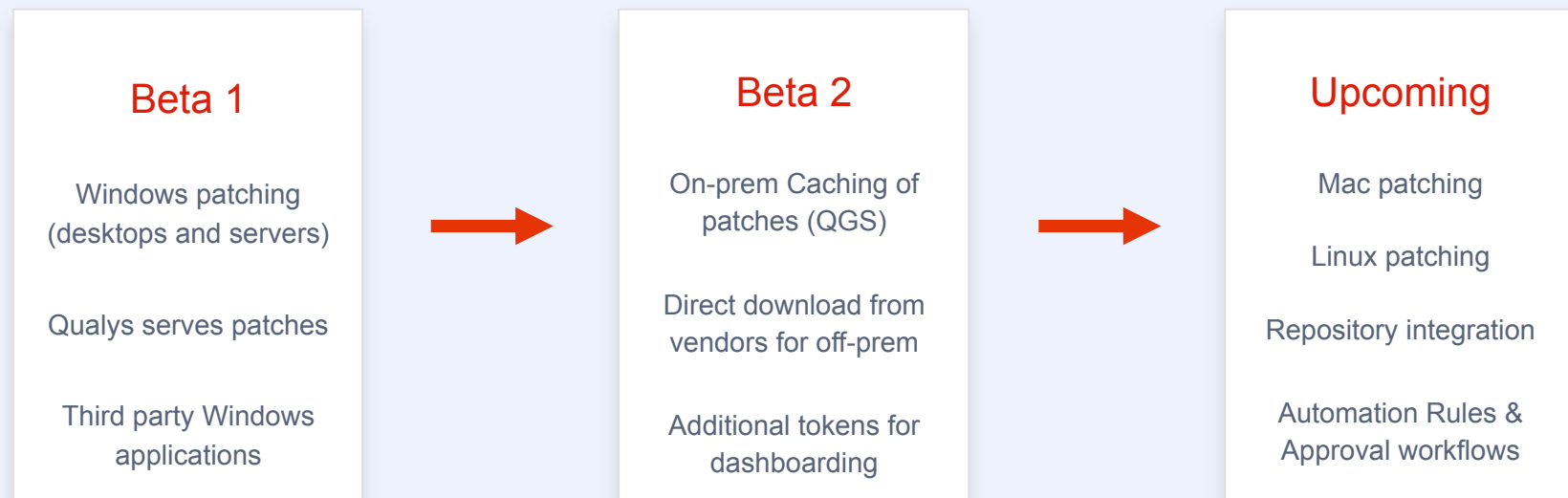
Ubuntu 14.x,15.x,16.x,
18.x

* Beta will focus on Windows- other operating systems will follow later

* Roadmap items are future-looking; timing and specifications may change

Roadmap

Beta: Q4 2018 – Windows patch deployment
General Availability: Early 2019





QUALYS SECURITY CONFERENCE 2018

Thank You

Michael Kassim
mkassim@qualys.com

Giorgio Gheri
ggheri@qualys.com